REMARKS

Applicants reply to the Office Action dated January 24, 200 within the shortened three month statutory period for reply. Claims 1-50 were pending in the application and claims 1, 14, 26 and 37 are independent. The Examiner rejects claims 1-50. Support for the amendments may be found in the originally-filed specification, claims, and figures. No new matter has been introduced by these amendments. Applicants respectfully submit that the application is in condition for allowance and request reconsideration of the pending claims.

The Examiner rejects claims 1-50 under first paragraph of 35 U.S.C 112 for antecedent issues and lack of support. Applicants respectfully traverse this rejection.

With respect to 7.1 in the Office Action, regarding the lack of support rejections on the three limitations introduced in claims 1-50, Applicants delete the term "contents" from "contents decryption device" and "contents encryption device," so these rejects are now moot.

With respect to 7.2 in the Office Action, the Examiner asserts that the limitation "wherein the contents decryption key is not required to be encrypted or decrypted by the decryption device" is not supported in the detailed description. The Examiner also asserts that it is unclear whether the decryption device is the same as the contents decryption device. Furthermore, the Examiner asserts that, if the devices are different components, it is unclear where the encrypted decryption key is decrypted and how it is delivered to the device performing the decryption.

Applicants assert that, with the amendments to the "content decryption device" to be "decryption device", the antecedent basis and clarity issues regarding the decryption device are now moot. Therefore, it will be clear that there is only a single decryption device. Applicants also assert that it is abundantly clear from the description that no encryption or decryption is required for the contents decryption key. In particular, the detailed description of the present application describes "The contents key generation section 118 generates the contents key CK from the decryption limitation S4 (S211). The encryption section 120 in the decryption device 102 decrypts the encrypted contents S5 using the contents key CK (S212)" (e.g., pages 25 lines 10-20 and Fig. 1). Moreover, the present invention discloses explicit encryption/decryption sections to be used when encryption/decryption is necessary (e.g., 113-116, 119-120 of Fig. 1). Specifically, encryption/decryption is only needed when content is to be transferred/received. Clearly, the content key CK generated and used in the decryption device 102 is never transferred.

Significantly, it is clear that it is the same content key CK that is generated and used in the decryption device without unnecessary encryption/decryption.

It is not mentioned, suggested or contemplated that any encryption/decryption should or would be performed. Applicants assert that it is inappropriate to assume that encryption/decryption steps are performed and a person skilled in the art would interpret as such from the disclosure of the present application. Therefore, the Examiner's concerns regarding where the decryption key is decrypted is not applicable as the decryption key was not encrypted in the first place. Moreover, the content key CK is generated in the decryption device. Significantly, the Examiner's concern regarding how the decryption key is delivered to the decryption device is not applicable as the decryption key is generated in the decryption device itself. Therefore, Applicants assert that such feature can be clearly understood from the disclosure of the present application. Consequently, the present rejection should be withdrawn.

With respect to 7.3 of the Office Action, the Examiner asserts that the limitation "time-varying keys not required to be transmitted to the contents decryption device" is not supported in the detailed description. The Examiner also asserts that no explicit disclosure exists in the present application that describes such feature. In addition, the Examiner has cited a new reference Frutiger to show that such feature was well-known at the time of invention.

Applicants assert that the presently claimed invention discloses the generation of the same time-varying key VK in both the encryption and decryption device. As such, the person of ordinary skill in the art would realize that such transfer is unnecessary from the disclosure of the present application. Applicants also assert that the cited references are not relevant to support the Examiner's rejections.

The Examiner next rejects claim 1 under 35 U.S.C. 103(a) as being obvious over Ishibashi (USP 6,728,379). The Examiner next rejects claims 2-50 under 35 U.S.C. 103(a) as being obvious over Ishibashi (USP 6,728,379) and further in view of Frutiger (USP 4,071,693). Applicants respectfully traverse these rejections.

The Examiner continues to maintain his obviousness rejection on claim 1. In response to our argument that the content keys do not need to be encrypted or decrypted since they are not required to be transferred and that the content keys disclosed in Ishibashi must be encrypted and decrypted since they must be transferred, the Examiner asserts that Ishibashi discloses that only the encrypted elements needed to generate the content keys are transferred and not the keys

itself. The Examiner likens such a feature to the transfer of encrypted decryption limitations of the present application.

In contrast, Applicants assert, as argued in our previous Reply, that the content keys of the present invention are not encrypted or decrypted. Similarly, Applicants do not agree with the Examiner's assertion that the transfer of encrypted/decrypted elements are used to generate such content keys. Ishibashi clearly discloses that the encrypted decryption key is transferred to the decryption device, and not just the elements used to generate the decryption key. Moreover, for security reasons, the content decryption key is encrypted before being transferred. Subsequently, the encrypted decryption key must be decrypted by the decryption device. (e.g., Fig 8, col. 5 lines 13-21, col. 6. lines 14-19, and col. 10 lines 27-32) It appears the Examiner has admitted to such deficiency when the Examiner states that "However, as mentioned above, Ishibashi's keys are not transferred in clear text either" (See section 3(2) of the present Office Action) and "However, the combination of the Kcd and the copy control code is an item that is generated based on the copy control code. That item is later encrypted by an encryption key (See col. 6 lines 1-20)" (See section 4 second paragraph of the Office Action dated August 6, 2007). Applicants assert that this is because the invention disclosed in Ishibashi requires the decryption key to be encrypted/decrypted. Applicants argued that the presently claimed invention does not require such restriction in our previous Reply; however, Applicants respectfully assert that the Examiner has failed to adequately address such deficiency. Moreover, the Examiner's lack of support rejection on such limitation is addressed with respect to the arguments about 7.3 of the Office Action above.

Applicants also do not agree with the Examiner's assertion regarding the generation of a content encryption key. Again, Applicants assert it is unreasonable and inappropriate to combine the features of the content provider 10 and the information processor 100. In particular, Applicants strongly assert that neither the content provider 10 nor information provider 100 would generate a content encryption key based on a second limitation obtained by updating a first limitation.

The Examiner alleges that the copy control function requires cooperation between the server side 10 and the user side 100 and that there would be motivation to combine such features since the content provider is interested in determining how many copies are to be made (See section 4 paragraph 3 of the Office Action dated August 6, 2007). However, Applicants

respectfully assert that the Examiner has not provided support on such cooperation between the server side 10 and user side 100. Referring to Fig. 8, Applicants assert that it can clearly be seen that the user side does not indicate transmitting any information to the server side 10. This is because the server side 10 is only disclosed to be supplying content to the user side (e.g., col. 3, lines 43-55). Even if the server side 10 was interested in determining how many copies are made, as argued by the Examiner, Applicants assert that it would not generate an encryption key based on such updated information. It is unclear why the content provider would generate an encryption key based on such updated information as there is already a content encryption key associated with the corresponding content (e.g., col. 4 lines 34-35, col. 5 lines 13-18, col. 8 lines 42-45). From Fig. 8, Applicants assert that it can clearly be seen that the encrypted content Kce(Cont) is used throughout. Additionally, Applicants assert that it would not make sense for content supplied to a user to be restricted by the copy control of content supplied to another user.

Furthermore, Applicants assert that Ishibashi only discloses the use of content encryption key Kce which is generated at the content provider 10 and does not mention generating encryption keys for encrypting content in the information processor 100. In fact, Applicants assert that Ishibashi teaches away from generating a new content encryption key in the information processor by using the stored encrypted content received from the content provider 10 when the content is needed to be transferred (e.g., col. 8 lines 8-11). Applicants also assert that Ishibashi further discloses that copy control code is added to the content decryption key Kcd which is then encrypted and sent to the information processor 200 (e.g., col. 12 lines 33-43). The information processor 100 than sends the encrypted content Kce(Cont) received from the content provider 10 to the information processor 200 where it is decrypted (e.g., col. 13 lines 16-28). This process disclosed by Ishibashi is used to reduce labor and time from decrypting and encrypting encrypted data which is to be transferred (e.g., col. 14 lines 2-11 and col. 14 lines 12-17). Hence, Applicants assert that the information processor 100 does not require a content encryption key and would not generate such a content encryption key.

Therefore, Applicants assert that neither the server side 10 nor the information processor 100 of Ishibashi would generate a content encryption key based on an updated limitation. As such, Applicants assert that for at least these reasons, the features of claim 1 are novel and inventive over Ishibashi and the present rejection should be withdrawn.

Claims 2-13 variously depend from independent claim 1, so Applicants assert that claims 2-13 are differentiated from the cited references for the same reasons as set forth above, in addition to their own respective features.

The Examiner maintained the rejection of claim 14. In particular, the Examiner has taken features of the content provider 10 and information processor 100 of DI to correspond to the features recited in claim 14. In addition, the Examiner relies on a new cited reference Frutiger to disclose the feature of not transmitting time-varying keys generated at the transmitter and receiver, which was introduced in Applicants' previous Reply. Therefore, the Examiner argues that the claimed invention of claim 14 is obvious.

Applicants traverse such rejection in the same manner as above regarding claim 1. In particular, Applicants assert that the feature of generating a content encryption key based on a second limitation obtained by updating a first limitation is not disclosed or contemplated by Ishibashi. As well, Applicants assert that Frutiger has not been found to make up for the deficiency of Ishibashi. In addition, Applicants amend claim 14, and its dependent claims to further define the contents key to be a contents encryption key for consistency with Claim 1. Support for such amendment can be found on, for example, page 25, lines 10-15.
Therefore, Applicants assert that such feature is not obvious from the disclosure of Ishibashi, Frutiger, nor any combination thereof, and the rejections on claim 14 should be withdrawn.

Claims 15-25 variously depend from independent claim 14, so Applicants assert that claims 15-25 are differentiated from the cited references for the same reasons as set forth above, in addition to their own respective features.

The Examiner maintained the rejection of claim 26. In particular, the Examiner asserts that the information processors 100 and 200 correspond to the decryption device of the present invention. Therefore, the Examiner argues that the claimed invention of claim 26 is obvious.

Applicants assert that claim 26 is differentiated from the cited references for the same reasons as set forth above for differentiating claim 1. In particular, the decryption key disclosed in Ishibashi is clearly encrypted, transmitted and decrypted. Ishibashi clearly discloses that the decryption key is encrypted in the encryption device 100 and transferred to the decryption device 200: "At step 5, the data is transmitted to the information processor 200. In this embodiment, a copy control code and content decryption key Kdc^{cx} are encrypted by an encryption key (session key Ksession)" (e.g., col. 13 lines 9-12). Moreover, the encrypted decryption key is decrypted

by the decryption device 200: "At step 6, the second information processor 200 sends the copy control code-added encrypted content decryption key Ksession(Kdc^{cx}") to the content decryption section 233 where it is decrypted by the session key Ksession to extract the content decryption key Kdc^{cx} having the copy control code inserted therein" (e.g., col. 13 lines 16-21). The same process is disclosed when considering the encryption and decryption device to be the content provider 10 and the information processor 100, respectively. E.g., col. 5 lines 18-21 and col. 5 lines 37-41.

Applicants assert that Frutiger has not been found to make up for the deficiency of Ishibashi. Applicants assert that, since it is clearly shown that the content decryption key of Ishibashi is encrypted, decrypted and transferred, such feature is novel and inventive over the prior art. Therefore, the present rejection on claim 26 should be withdrawn for at least the reasons above.

Claims 27-36 variously depend from independent claim 26, so Applicants assert that claims 27-36 are differentiated from the cited references for the same reasons as set forth above, in addition to their own respective features.

Claim 37 recites a recording medium storing a program which communicates with an encryption device. Such program stored on a recording medium acts as a decryption device. Applicants assert that claim 37 is differentiated from the cited references for the same reasons as set forth above for differentiating claim 26. In addition, Applicants amend claim 37 to more closely reflect the recitation of claim 26. In particular, Applicants amend claim 37 to recite: "contents decryption key" and "wherein the contents decryption key is not required to be transferred to or from the encryption device and is not required to be encrypted or decrypted;". Applicants assert that neither Ishibashi, Frutiger, nor any combination thereof, teach or suggest such feature as explained in the argument regarding claim 26 above. Therefore, since claim 37 also recites such feature, the rejection on claim 37 should be withdrawn.

Claims 38-50 variously depend from independent claim 37, so Applicants assert that claims 38-50 are differentiated from the cited references for the same reasons as set forth above, in addition to their own respective features.

In view of the above remarks, Applicants respectfully submit that all pending claims properly set forth that which Applicants regard as their invention and are allowable over the cited reference. Accordingly, Applicants respectfully request allowance of the pending claims. The

Examiner is invited to telephone the undersigned at the Examiner's convenience if it would help further prosecution of the subject Application. The Commissioner is authorized to charge any fees due to Deposit Account No. 19-2814.

Respectfully submitted,

Dated: April 22, 2008

Howard J. Sobelman
Reg. No. 39,038

SNELL & WILMER L.L.P.
400 E. Van Buren
One Arizona Center
Phoenix, Arizona 85004
Phone: 602-382-6228
Fax: 602-382-6070
Email: hsobelman@swlaw.com